APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/994,919	11/28/2001	Winston Donald Keech	46354.010500	7412

22191   7590   08/02/2007
GREENBERG TRAURIG, LLP
1750 TYSONS BOULEVARD, 12TH FLOOR
MCLEAN, VA 22102

EXAMINER
DOAN, TRANG T

ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
08/02/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

kinneyb@gtlaw.com
tcopatdkt@gtlaw.com
goepelj@gtlaw.com

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 July 2007*.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-12,14-17 and 19-27* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-12,14-17 and 19-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 March 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

U.S. Patent and Trademark Office

PTOL-326 (Rev. 08-06)   Office Action Summary.   Part of Paper No./Mail Date 20070726

DETAILED ACTION

1.   This action is in response to the amendment filed on 05/23/2007.

2.   Claims 1, 3, 9, 11-12 and 15-17 have amended. Claims 2, 13 and 18 have

canceled. Claims 1, 3-12, 14-17 and 19-27 are pending for consideration.

Continued Examination Under 37 CFR 1.114

3.   A request for continued examination under 37 CFR 1.114, including the fee set

forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

application is eligible for continued examination under 37 CFR 1.114, and the fee set

forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on

05/23/2007 has been entered.

Response to Arguments

4.   Applicant's arguments with respect to claims 1, 3-12, 14-17 and 19-27 have been

considered but are moot in view of the new ground(s) of rejection.

Double Patenting

5.   The nonstatutory double patenting rejection is based on a judicially created
doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the
unjustified or improper timewise extension of the "right to exclude" granted by a patent
and to prevent possible harassment by multiple assignees. A nonstatutory
obviousness-type double patenting rejection is appropriate where the conflicting claims
are not identical, but at least one examined application claim is not patentably distinct
from the reference claim(s) because the examined application claim is either anticipated
by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140

F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29
USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir.
1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422
F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163
USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d)
may be used to overcome an actual or provisional rejection based on a nonstatutory
double patenting ground provided the conflicting application or patent either is shown to
be commonly owned with this application, or claims an invention made as a result of
activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a
terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with
37 CFR 3.73(b).

6.   Claims 1, 9, 12, 15, 16-17 and 25 are rejected on the ground of nonstatutory

obviousness-type double patenting as being unpatentable over claims 1, 7-8 and 18 of

U.S. Patent No. 7043635 (hereinafter Keech) in view of Marvit et al (US 6625734)

(hereinafter Marvit). Keech discloses verification communication between the two

computer, wherein the identity of a first user is verified and characters selected from a

first array and second array form a volatile identification code, which is a third array.

Keech does not disclose encryption method. Marvit discloses encryption method

(Marvit: see figures 1 and 8). Therefore, it would have been obvious to one ordinary

skill in the art at the time the invention was made to modify the procedure in Keech by

including encryption method as taught by Marvit, because such modification would

provide the procedure in Keech with a comprehensive approach for controlling and

tracking access to data disseminated on communications networks (Marvit: column 2

lines 3-5).

Claim Comparison Table

Instant Application 09/994919	Patent Application 7043635
Claims 1, 12, 16 and 17. A method of	**Claims 1, 7, 8 and 18**. A coded

transferring a data file having a file name from a first computer operated by a first user to a second computer operated by a second user, wherein the method is performed under control of a third computer, comprising: a) permitting the first user to select, on the first computer, a data file which is to be transferred; b) establishing a communications link between the first computer and the third computer; c) verifying an identity of the first user to the third computer by way of verification communications between the first and third computers, wherein the identity of the first user is verified by way of: **generating, in the third computer, a pseudo-random security string**; transmitting the pseudo-random security string from the third computer to the first computer; causing the first computer to display the pseudo-random security string to the first user; permitting the first computer to receive from the first user a volatile identification code, **wherein the first user volatile identification code is created by the user applying a first user mask code to the pseudo-random security string**; transmitting the first user volatile identification code from the first computer to the third computer and causing the third computer to **compare the first user volatile identification code with a first check volatile identification code obtained by applying the first user mask code to the pseudo-random security string in the third computer, wherein the identity of the first user is verified when the user volatile identification code and the first check volatile identification codes are found to match** each other.

Claims 9, 15 and 25. wherein: i) the pseudo- random string comprises a first

identification system, the system comprising an electronic computer, a specific electronic communications device that is operable to be in communication with the electronic computer, and at least one electronic communications device that is operable to be in communication with the electronic computer, wherein the electronic computer includes data relating to the specific electronic communications device, including a permanent identification code, a mask code and an identification code enabling electronic communication between the electronic computer and the specific electronic communications device, and wherein the permanent identification code is input to the at least one electronic communications device and transmitted to the electronic computer, **the electronic computer generates a pseudo-random string and transmits this to the specific electronic communications device, the mask code is applied to the pseudo-random string so as to generate a volatile identification code** in accordance with predetermined rules, the volatile identification code is transmitted back to the electronic computer by the specific electronic communications device or the at least one electronic communications device, **the electronic computer checks the volatile identification code transmitted thereto against a volatile identification code obtained by applying the mask code to the pseudo-random string in accordance with the predetermined rules, and in which a positive identification is made when the volatile identification codes are found to match by the electronic computer**, wherein the pseudo-random string comprises a first array of characters; **each character having a given numerical**

| linear array of characters, **each character having a given numerical position in the first array** (first, second, third etc.); ii) the mask code comprises **a second linear array of numbers, each number having a given numerical position in the second array** (first, second, third etc.); and iii) the volatile identification code is **generated by applying the mask code to the pseudo-random string so as sequentially to select numerical positions in the first array on the basis of the numbers in the second array, taken in positional order**, and to return the characters thereby selected from the first array in sequence so as to form a third linear array, **this third linear array forming the volatile identification code.** | **position in the first array** (first, second, third etc.), and wherein the mask code comprises **a second array of numbers, each number having a given numerical position in the second array** (first, second, third etc.), the predetermined rules for applying the mask code to the pseudo-random string so as to **generate the volatile identification code being sequentially to select numerical positions in the first array on the basis of the numbers in the second array, taken in positional order**, and to return the characters thereby selected from the first array in sequence so as to form a third array, this **third array forming the volatile identification code.** |

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8.   Claims 1, 3-7, 10-12, 16-17, 19-23 and 26-27 are rejected under 35

U.S.C. 103(a) as being unpatentable over Ishikawa et al. (US 6343284) (hereinafter

Ishikawa) in view of Marvit et al. (US Patent 6625734) (hereinafter Marvit).

9.   Regarding claim 1, Ishikawa discloses a) permitting the first user to select, on the

first computer, a data file which is to be transferred (Ishikawa: see Summary section); b)

establishing a communications link between the first computer and the third computer

(Ishikawa: see figure 5); c) verifying an identity of the first user to the third computer by

way of verification communications between the first and third computers, wherein the

identity of the first user is verified by way of: generating, in the third computer, a

pseudo-random security string; transmitting the pseudo-random security string from the

third computer to the first computer; causing the first computer to display the pseudo-

random security string to the first user; permitting the first computer to receive from the

first user a volatile identification code, wherein the first user volatile identification code is

created by the user applying a first user mask code to the pseudo-random security

string; transmitting the first user volatile identification code from the first computer to the

third computer and causing the third computer to compare the first user volatile

identification code with a first check volatile identification code obtained by applying the

first user mask code to the pseudo-random security string in the third computer, wherein

the identity of the first user is verified when the user volatile identification code and the

first check volatile identification codes are found to match each other (Ishikawa: see

Summary section and column 3 lines 3-20).

However, Ishikawa does not specifically disclose in detail encrypting the data file

from a first computer, transmitting the executable file containing the encrypted data file

to the second computer from the first computer, establishing a communication link

between the second computer and the third computer, verifying an identity of the

second user, transmitting the file name of the data file from the second computer to the

third computer with a request for unique key code, and transmitting the unique key code

from the third computer to the second computer to decryption the data file.

Marvit discloses encrypting the data file from a first computer, transmitting the

executable file containing the encrypted data file to the second computer from the first

computer, establishing a communication link between the second computer and the

third computer, verifying an identity of the second user, transmitting the file name of the

data file from the second computer to the third computer with a request for unique key

code, and transmitting the unique key code from the third computer to the second

computer to decryption the data file (Marvit: see figure 1 and figure 8 and column 12

line 54 through column 13 line 2). Therefore, it would have been obvious to one

ordinary skill in the art at the time the invention was made to modify the procedure in

Ishikawa by including encryption method as taught by Marvit, because such

modification would provide the procedure in Ishikawa with a comprehensive approach

for controlling and tracking access to data disseminated on communications networks

(Marvit: column 2 lines 3-5).

10.   Regarding claim 3, Ishikawa discloses wherein the identity of the second user is

verified in step viii) above by way of the second user applying a second user mask code

to a first pseudo-random security string in the second computer so as to generate a

second user volatile identification code, the second user transmitting the second user

volatile identification code to the third computer and the third computer comparing the

second user volatile identification code with a second check volatile identification code

obtained by applying the second user mask code to a second pseudo-random string in

the third computer, identity verification taking place when the second user volatile

identification code and the second check volatile identification codes are found to match each other (Ishikawa: see Summary section and column 3 lines 3-20).

11.   Regarding claim 4, Ishikawa discloses wherein the first pseudo-random security string and the second pseudo-random security string are the same (Ishikawa: see Summary section).

12.   Regarding claim 5, Ishikawa discloses wherein the pseudo-random string is generated by the third computer and transmitted firstly to the first computer and then from the first computer to the second computer (Ishikawa: see figure 1 and Summary section).

13.   Regarding claim 6, Ishikawa discloses wherein the pseudo-random string is generated by the third computer and transmitted firstly to the first computer and then from the third computer to the second computer (Ishikawa: see figure 1 and Summary section).

14.   Regarding to claim 7, Ishikawa discloses wherein the first pseudo-random security string and the second pseudo-random security string are different (Ishikawa: see figure 1 and Summary section).

15.   Regarding to claim 10, Ishikawa does not explicitly disclose in detail wherein the third computer maintains a record of transactions between the first, second and third computers so as to permit an audit trail to be established. Marvit discloses wherein the third computer maintains a record of transactions between the first, second and third computers so as to permit an audit trail to be established (Marvit: column 3 lines 11-56). Therefore, it would have been obvious to one ordinary skill in the art at the time the

invention was made to modify the procedure in Ishikawa by including the record of

transactions between the first, second and third computers so as to permit an audit trail

to be established as taught by Marvit, because such modification would provide the

procedure in Ishikawa with a comprehensive approach for controlling and tracking

access to data disseminated on communications networks (Marvit: column 2 lines 3-5)..

16.   Regarding to claim 11, Ishikawa does not explicitly disclose in detail wherein the

first and/or second user volatile identification codes are stored as digital signatures in

the third computer in combination with the associated pseudo-random security string.

However, Marvit discloses wherein the first and/or second user volatile identification

codes are stored as digital signatures in the third computer in combination with the

associated pseudo-random security string (Marvit: column 17 lines 42-59). Therefore, it

would have been obvious to one ordinary skill in the art at the time the invention was

made to modify the procedure in Ishikawa by including user volatile identification codes

are stored as digital signatures as taught by Marvit, because such modification would

provide the procedure in Ishikawa with a comprehensive approach for controlling and

tracking access to data disseminated on communications networks (Marvit: column 2

lines 3-5).

17.   Regarding to claim 12, this claim has limitations that is similar to those of claim 1,

thus it is rejected with the same rationale applied against claim 1 above.

18.   Regarding to claim 16, this claim has limitations that is similar to those of claim 1,

thus it is rejected with the same rationale applied against claim 1 above.

19.   Regarding to claim 17, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

20.   Regarding to claim 19, the rejection of claim 18 is incorporated and further this claim has limitation that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

21.   Regarding to claim 20, the rejection of claim 19 is incorporated and further this claim has limitation that is similar to those of claim 4, thus it is rejected with the same rationale applied against claim 4 above.

22.   Regarding to claim 21, the rejection of claim 20 is incorporated and further this claim has limitation that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above.

23.   Regarding to claim 22, the rejection of claim 20 is incorporated and further this claim has limitation that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

24.   Regarding to claim 23, the rejection of claim 19 is incorporated and further this claim has limitation that is similar to those of claim 7, thus it is rejected with the same rationale applied against claim 7 above.

25.   Regarding to claim 26, the rejection of claim 17 is incorporated and further this claim has limitation that is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

26.   Regarding to claim 27, the rejection of claim 18 is incorporated and further this claim has limitation that is similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 above.

27.   Claims 8, 14 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishikawa in view of Marvit, and further in view of Wilfong U.S. Patent 5754652 (hereinafter Wilfong).

28.   Regarding to claim 8, Ishikawa in view of Marvit does not explicitly disclose:

i) said secure user code entry interface contains at least one active display for entry of at least one digit of said user mask code by the user; wherein said active display illuminates or highlights at least one display digit within said active display and said user enters said at least one digit of said user mask code by a response through an input device at a response time when said at least one display digit which corresponds with said at least one digit of said user mask code is illuminated or highlighted in said active display; and

ii) a random run on time is added to said response time to extend said at least one active display.

However, Wilfong teaches i) said secure user code entry interface contains at least one active display for entry of at least one digit of said user mask code by the user; wherein said active display illuminates or highlights at least one display digit within said active display and said user enters said at least one digit of said user mask code by a response through an input device at a response time when said at least one display digit which corresponds with said at least one digit of said user mask code is

illuminated or highlighted in said active display (Wilfong: column 2 lines 28-41); and ii) a

random run on time is added to said response time to extend said at least one active

display (Wilfong: column 2 lines 28-41).

At the time of the invention, it would have been obvious to one ordinary skill in

the art at the time the invention was made to modify the procedure in Ishikawa in view

of Marvit by including active display illuminates or highlights at least one display digit

within said active display as taught by Wilfong, because such modification would

provide the procedure in Ishikawa in view of Marvit with verifying user's identity by using

an active display to capture the PIN number of user at a response time because the

system prompts are made in such a way as not to be observable by bystanders

(Wilfong: column 2 lines 32-34).

29.   Regarding to claim 14, the rejection of claim 12 is incorporated and further this

claim has limitations that is similar to those of claim 8, thus it is rejected with the same

rationale applied against claim 8 above.

30.   Regarding to claim 24, the rejection of claim 17 is incorporated and further this

claim has limitations that is similar to those of claim 8, thus it is rejected with the same

rationale applied against claim 8 above.

31.   Claims 9, 15 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Ishikawa in view of Marvit, and further in view of Covert (US 5177789) (hereinafter

Covert).

32.   Regarding to claim 9, Ishikawa in view of Marvit does not explicitly disclose:

i) the pseudo-random string comprises a first linear array of characters, each character having a given numerical position in the first array (first, second, third etc.);

ii) the mask code comprises a second linear array of numbers, each number having a given numerical position in the second array (first, second, third etc.); and

iii) the volatile identification code is generated by applying the mask code to the pseudo-random string so as sequentially to select numerical positions in the first array on the basis of the numbers in the second array, taken in positional order, and to return the characters thereby selected from the first array in sequence so as to form a third linear array, this third linear array forming the volatile identification code.

However, Covert teaches that limitation (Covert: see figures [5, 6] and column 5 lines 15-46). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention to apply the teaching of Covert to the system of Ishikawa in view of Marvit because it would provide the benefit of using a computer security device and method in which both an encrypted password and an encrypted time-related code are required for access to a computer system, wherein the information is generated employing a small, easily carried, simple and inexpensive device (Covert: column 2 lines 10-14).

33.   Regarding to claim 15, the rejection of claim 13 is incorporated and further this claim has limitation that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

34.   Regarding to claim 25, the rejection of claim 18 is incorporated and further this claim has limitation that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Trang Doan whose telephone number is (571) 272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Trang Doan
Examiner
Art Unit 2131

T.D.

CHRISTOPHER REVAK
PRIMARY EXAMINER